USAWC STRATEGY RESEARCH PROJECT

SECURING AMERICAN CYBERSPACE: A STRATEGIC NECESSITY

by

Lieutenant Colonel James E. Barrineau
United States Army

Colonel David J. Smith
Project Advisor

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
03 MAY 2004		**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Securing American Cyberspace: A Strategic Necessity	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
James Barrineau	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
U.S. Army War College,Carlisle Barracks,Carlisle,PA,17013-5050	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached file.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**38**	

ABSTRACT

AUTHOR: LIEUTENANT COLONEL JAMES E. BARRINEAU

TITLE: SECURING AMERICAN CYBERSPACE: A STRATEGIC NECESSITY

FORMAT: Strategy Research Project

DATE: 19 March 2004 PAGES: 38 CLASSIFICATION: Unclassified

United States (U.S.) cyberspace is not secure, and this lack of security leaves the nation vulnerable to cyberattack from a variety of sources. Successful cyberattacks have had, and may continue to have, negative results with strategic implications. Until now cyberspace has existed with relatively unregulated access. However, as the reliance on cyberspace grows, the subsequent requirement for security also grows with it, and we must now take at least the minimum necessary measures to better secure it, or continue to suffer the consequences of computer attacks from a variety of threats. The U.S. Government must first set the example by securing itself, and then move to bring industry into compliance, preferably through consensus, but if necessary, through regulation or legislation. While government should display the necessary leadership in this arena, industry has the great majority of the nation's infrastructure, and therefore will bear the largest burden. Finally, individual users must take a more active role in securing their small part of cyberspace. All three have a key role in securing American cyberspace in order to prevent a potential "digital Pearl Harbor" or "electronic September 11" from ever occurring.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

Thanks to my Faculty Advisor, David J. Smith, Colonel, U.S. Army, for his advice and counsel. He put this Strategic Research Project in its proper perspective, provided me a framework within which to research, study, learn, and then write about cyberattacks. In the end I was very pleased with the results.

Further thanks to Mr. Ron Stewart, Deputy Director of the U.S. Army Network Enterprise and Technology Command's (USANETCOM) Continental U.S. Theater Network Operations and Security Center (CONUS-TNOSC) at Fort Huachuca, Arizona. During my time as director, no one could have asked for a better deputy, and no one probably knows more about Computer Network Operations (CNO) in the U.S. Army than he does.

I also am fortunate to have had Richard (Rick) Howard, Lieutenant Colonel (Promotable), U.S. Army, for his input. When I wrote this paper, he was the Director of the U.S. Army Computer Emergency Response Team (USACERT), of the U.S. Army's 1st Information Operations Command at Fort Belvoir, Virginia. I doubt there are any officers in the military today that know more about Computer Network Defense (CND).

I am indebted to my father-in-law, Dr. Charles C. Holt, Ph.D., and Professor Emeritus. His contributions to this paper forced it to a higher plane of excellence than I could ever have imagined on my own.

Finally, thanks to my family; my wife Hilary, my sons Holt and Hunter. It all begins and ends with you. Everything in the middle is just filler.

SECURING AMERICAN CYBERSPACE: A STRATEGIC NECESSITY

> There's been speculation, even before September 11, about the U.S.'s vulnerability to an "electronic Pearl Harbor" or a cyberterrorist attack.[1]

U.S. cyberspace[2] is not secure, and this lack of security leaves the nation vulnerable to cyberattack from a variety of sources. Successful cyberattacks have had, and may continue to have, negative results with strategic implications.[3] Therefore, this paper has three purposes; first, to define the cyber threat; second, to analyze why the U.S. is vulnerable to cyberattack and the reasons we are still susceptible to attacks; and finally, to recommend potential solutions for improving the nation's cybersecurity.

THE THREAT

Three major threats to American cyberspace exist today: cybercrime, cyberterrorism, and state-sponsored cyberattacks. Cybercrime is criminal activity conducted in cyberspace; that activity, whether intentionally or unintentionally, which directly attacks another computer, information system, or network, causing them to be disrupted, their services denied, or in the worst case causing equipment damage or loss of services to the user of the system. Specific examples are hacking, website defacements (cybervandalism,) and cyberfraud (i.e., stock manipulations or illegal bank account "break ins"). However, the historically most dangerous is malicious code, of which the computer virus[4], with its variants the worm and Trojan horse, is the best known. Cybercrime has cost government and business billions of dollars.[5]

Cyberterrorism has received a lot of more attention since September 11. According to the Federal Bureau of Investigation, cyberterrorism is any "premeditated, politically motivated attack against information, computer systems, computer programs and data which results in violence against non-combatant targets by sub-national groups or clandestine agents."[6] A big fear is that a cyberterrorist could shut down the Internet, causing significant damage to the economy (not unlike the physical attacks of September 11), as well as attack key infrastructure such as oil, gas, power, and emergency services.[7]

State-sponsored threats, using cyberattack as a form of asymmetric warfare, in conjunction with direct physical attacks, are of even greater concern. Asymmetric warfare is "anything that encompasses anything—strategy, tactics, weapons, personnel—that alters the battlefield to negate one side or the other's advantages."[8] Because the U.S. is a superpower today without a military peer adversary, no potential enemy since the end of the Cold War has demonstrated the ability to compete in a face-to-face conventional or "symmetrical" battle.

Therefore, the U.S. can expect that future enemies will attack using asymmetric threats, such as computer espionage and direct cyberattack, clandestinely launched, possibly through sympathetic cyberterrorists or mercenary hackers in their employ. While there is much debate over whether a nation can be brought to its knees via cyberattack, the second- and third-order effects, when synchronized in coordination with physical attack, could be devastating. At the very least they could hamper response times and the ability to recover from a military or terrorist assault. The consequence of such a combined attack might prove more devastating as its effects ripple through the global economy.

THE VULNERABILITY

Compelling evidence shows that American cyberspace is not fully secured. The Carnegie Mellon Software Institute's CERT (Computer Emergency Response Team) Coordination Center is recognized as a leader in computer network defense.[9] Its website lists the total number of reported computer network attack incidents in its 15-year history starting in 1988 and extending through calendar year 2003 (see Figure 1 below).[10] Since 1988 there have been 319,992 reported incidents of computer attack in various forms. The website states that each "incident may involve one site or hundreds (or even thousands) of sites. Also, some incidents may involve ongoing activity for long periods of time." In 2003 alone there were 137,529 incidents. This is over 42% of all reports ever.[11] Compared to the 82,094 reported in 2002, this is an increase of almost 75% over the year before. When compared to the 21,756 reported incidents of 2000, this further represents a greater than 600% increase in reported attacks since the Bush administration entered office. The Department of Defense (DOD) alone defended itself from over 50,000 reported attacks in 2002.[12]

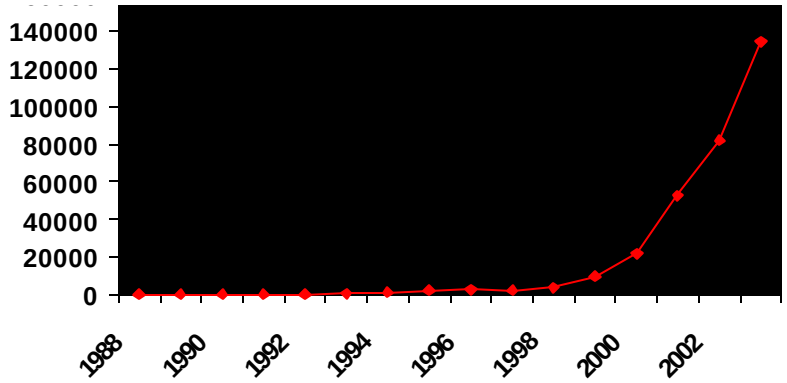

FIGURE 1. REPORTED COMPUTER ATTACK INCIDENTS 1988-2003

The government has a $52 billion-a-year information technology (IT) budget and in 2002 spent $4.5 billion on IT security, a 64% increase from the year before.[13] Depending on which report one believes, the government owns 10% to 20% of U.S. cyberspace.[14] Using 15% as an estimating figure (simply averaging between 10% and 20%), and extrapolating government security expenditure to corporate America, the latter spends about $346 billion a year on IT, of which approximately $29 billion is on IT security.[15] Yet reports of network attacks have grown over 600% since 2000. While one could expect that attacks would increase as the usage in cyberspace grows, if security measures were working one should also expect successful attacks to decrease. Either enough is not being spent, or there is not enough capability to keep up. Both are likely true, with security spending lagging behind that which is required to defend cyberspace, regardless of the advance of technology.

The consequences of a lapse in cybersecurity, or not keeping pace with security upgrades as new threats emerge, can be extremely expensive as well. In late summer of 2003, a wave of viruses caused an estimated $3.5 billion in damage.[16] If cyberspace users think it costs a lot to secure their systems, the cost of not securing them could be substantially higher.

In comparison, for the price of just a few hundred dollars, a cyberattacker can purchase late-model computer equipment and conduct direct attacks. More likely an attacker will release a virus "into the wild"[17] that indiscriminately attacks a majority of systems in cyberspace, causing particular targeted systems to fail, but usually via denial of service (DoS) attacks.[18] The rapid pace of technology works against the defender, but favors the attacker. Costs for cybersecurity can be seen as almost prohibitive if not for the fact that access to cyberspace today is a necessity, and security expenditures a "necessary evil." Essentially, even after government and corporations have spent millions of dollars to secure cyberspace worldwide, a single individual's minimal costs in personal equipment can be used to cause systems to crash causing billions in clean-up and lost productivity[19]. So despite significant monies spent, U.S. cyberspace still remains inadequately secured.

GOVERNMENT IS RESPONSIBLE

There are some key reasons why American cyberspace is still not secured. To start, the U.S. Government has not fully accepted its responsibility to secure it. When the Bush administration released *The National Strategy to Secure Cyberspace,* critics were quick to comment. An editorial by Silicon Valley's *San Jose Mercury News* on the advent of the National Cyber Security Summit several months after the strategy's release stated:

> The national strategy is a watered down document that relies almost exclusively on voluntary measures, education and awareness. Industry groups fought hard

> to keep it free of mandates. There are no requirements for basic security measures, disclosure or information sharing. There are no demands for cooperation between industry and government. And there are no real incentives to spend resources on making networks more secure and no consequences for failing to do so.[20]

The execution of the strategy after its release has been delayed, and billions of dollars for cybersecurity have not been spent. [21] Additionally, the newly formed Department of Homeland Security (DHS) has been busy organizing itself. As a result, while DHS was supposed to be ensuring that the strategy was being implemented, it lacked the ability to focus on this particular task. Additionally, the resignation of two cybersecurity directors in rapid succession left it without leadership to push the strategy forward.[22]

Interestingly, the "watered down" strategy deflected responsibility away from government and industry, placing an undue responsibility on individuals. While individual operators have a role to play, chances are they are not paying attention to the national cyber strategy. Russ Cooper, an executive with the Reston-based TruSecure Corporation, was quoted as saying, "Most consumers didn't buy a computer to become geeks. The majority of them are still trying to buy things from eBay." [23]

Government's push on the national strategy has been to gain consensus from the private sector on implementing the way ahead, much like the Clinton administration did for its Y2K plan.[24] However, in comparison toY2K, government made three key mistakes with its cyber strategy.

First, during preparation for the Y2K rollover, government planners made sure to float the plan among industry officials so that they built consensus as the plan progressed.[25] Unfortunately, this same process did not occur with the nation's cyber strategy until just before it was published. Consequently, many in industry balked at its recommendations, causing the current administration to back off, thus providing many voluntary measures with few volunteers.[26]

Next, government has not led the cybersecurity effort as it did during Y2K, by fixing itself first before insisting that others follow suit. Prior to the Y2K rollover, government demonstrated that it took Y2K seriously by examining all internal systems to ensure Y2K compliance. Where it was not compliant, it upgraded or fixed them to ensure that on January 1, 2000, government would not stop functioning. Much to government's credit, the end result was what many said was the biggest non-event in computer history. [27]

However, in contrast, considering the effect and cost of four recent viruses on cyberspace, Slammer ($1.2 billion); Code Red ($2.6 billion); LoveLetter ($8.8 billion), and Klez ($9.0

billion);[28] these can hardly be dismissed as non-events in cyberspace. Further, while it appears that the power blackout that affected the northeast this past August 2003 was not caused by a cyberattack, there is increasing evidence that the Blaster worm plowing through cyberspace at the same time may have inhibited power companies' recovery from the blackout.[29] This should put everyone on guard.

Knowing full well when the national cyber strategy was produced that cyberattacks have cost billions, at the end of 2003 government was still waiting for industry to do something. How long does the nation wait…until the "electronic Pearl Harbor" or "cyber September 11" hits? America went to war on a global scale when the physical versions of these two attacks occurred. Arguably, those who have operated within cyberspace for the last few years know that cyberwar has been in effect for some time. Perhaps the National Cyber Security Summit, which met in December 2003,[30] will produce the required synergy to finally move the country ahead to a more secure cyberspace. The concern is that the next dangerous attack may get here before then, and all government will be able to do is watch and react because it has not been more proactive.

INDUSTRY IS RESPONSIBLE

A greater reason cyberspace is not more adequately secured is that corporate America has not taken effective action. With 80% to 90% of the nation's cyber infrastructure, the high-tech industry lobbied intensely against mandatory security regulations very early during the Bush administration's writing of its cyber strategy.[31] Industry claimed mandatory measures would be too costly, especially in light of the recent downturn in the economy,[32] insisting market forces would drive them to choose the path of best security. The Bush administration's cyber strategy had plenty of recommendations on how home users should protect their systems, but critics complained lobbying done by tech companies "pulled nearly all the teeth" from the plan when it came to telling companies what they needed to do to protect themselves, omitting several recommendations contained in earlier drafts.[33]

This should not be surprising. Industry has resisted efforts by the government to regulate cyberspace since the Internet took shape. Recent debates in the Congress, in the media and the industry itself over the topic of taxation of cyberspace have been another touchy subject.[34] The Internet is looked at since its creation as a free-market medium in which not only the trade of goods but ideas is encouraged, and its users see any government regulation as an affront. Here at home, the government's cyber strategy has sought this *laissez faire* approach to

cyberspace,[35] depending on industry to take voluntary security actions,[36] though government's patience may be wearing thin.[37] [38]

Unfortunately, cyberspace has developed a dark side, where behaving badly has increased proportionate to the good; and while most users are benign, one malignant individual can make things unpleasant for the rest.[39] Nonetheless, it is understandable that industry would resist government regulation that takes away from the bottom line. They argued prior to the release of the national cybersecurity strategy that they be allowed time to increase security before dealing with government regulations.[40] Yet since the release of the national cybersecurity strategy, attacks are up, costing American cyberspace users billions. Clearly, industry has not been able to provide the security they stated they would, assuming they could.

This has gotten the attention of the federal government. During the cybersecurity summit hosted by four pro-business organizations in early December 2003, in Silicon Valley, and attended by DHS Secretary Tom Ridge, the government's message to the tech industry was clear: much still needs to be done, and industry needs to get serious about network security or face legislation.[41] Robert Liscouski, Assistant Secretary for Infrastructure Protection, was quoted at a press conference during the summit as saying, "There should be no mistake about where we stand. We are not going to let anybody who operates in this space dodge their responsibility, and I will be sticking my finger into people's chests to make sure they live up to their responsibilities."[42] Amit Yoran, the recently appointed director of the National Cyber Security Division at DHS was also quoted as saying, "The National Strategy didn't call for specific pieces of legislation. That does not mean, however, there is no role for legislation."[43] So it would seem the U.S. Government is losing patience with industry on its slow pace of cybersecurity. DHS has made the security of the Internet and e-commerce a top priority, and as Secretary Ridge stated in his keynote speech at the summit, "Terrorists know that a few lines of code could, ultimately, wreak as much havoc as bombs."[44] The signal to industry involved in e-commerce and cyberspace should be clear; after winning an initial reprieve from government intervention mandating better cybersecurity, government is sending a strong message to corporate America to get serious about it or intervention might soon follow.[45]

What remains to be seen is whether industry responds. It has not to this point, or successful computer attacks would be decreasing, along with their adverse effects. At the very least, successful attacks should not be growing at the rate they are. While industry has formed its own organizations to look at cybersecurity, [46] and owns over 80% of the country's cyber infrastructure, the infrastructure is very complex; and its ownership is spread among many companies. Can industry enact voluntary standards to enhance security of networks and the

information traveling them, especially when the network is only as strong as its weakest link[47]…without government intervention? It remains to be seen. At the very least, assuming industry moves fairly quickly in the right direction, it may require government to help enforce the standards which industry creates. The bigger question may turn out to be who will enforce the standards and discipline those who do not cooperate? Enforcement has usually been a governmental responsibility, and a requirement for governmental codifying of the standards through regulation or legislation may be necessary.

The working groups formed during the National Cyber Security Summit in December 2003, have a self-imposed deadline of March 1, 2004,[48] to produce white papers outlining their recommendations; so at the time of this writing the question of whether industry can respond remains unanswered. Even then, these recommendations will have to translate into action, and the question will still remain if industry, without the impetus of government enforcement, can really make them work. So far, the lack of government impetus has not. In the meantime, American cyberspace remains vulnerable.

INDIVIDUALS ARE RESPONSIBLE

Another reason for the lack of cybersecurity in America is the individual American computer user, at home and at work. Unfortunately, most computer users are ignorant about what is going on "under the hood" of their personal computer (PC). The first computer processor developed for personal computers was Intel's 8088[49] in June 1979. The very first version of the 8088 had a speed of 4.77 MHz (million cycles per second). Today, one can purchase a PC with a processor speed of over 3 GHz (billion cycles per second). So in 25 years, processor speed has increased over 628-fold.

Why is this important? As quoted before, the average traveler in cyberspace is more interested in learning to buy from eBay than conducting cyberattacks. Nonetheless, an unprotected computer is an opportunity for a cyberattacker to exploit without the computer user's knowledge. Despite the possible harvesting of sensitive information such as social security and credit card numbers, the more dangerous problem is the Zombie,[50] a computer exploited without the owner's knowledge, and then used to attack other computers or cyberspace at large, thus hiding the attacker's identity. The most prolific problem is the unprotected computer infected by a virus which then propagates itself back out into cyberspace at a rapid rate, causing DoS attacks.[51]

While the rate of computing power since the first PC chip was produced has gone up exponentially, and the number of computers has increased proportionally, so has the

operational ease of computers for the average user. Arguably, anyone of reasonable intelligence can operate a modern computer. However, while the early PCs were simple by today's standards, computers have become quite sophisticated and efficient instruments. Not only does the basic user not fully comprehend the power at his fingertips, he also does not fully appreciate the power of an attacker who does. Therefore, can the everyday user continue to remain unaware of the potential power to do ill if an attacker corrupts his computer? It may be time for both government and industry to step in to help the user be safer, much the way it did with the advent of the automobile and airplane over a hundred years ago. Historically, Big Brother stepping in to "help" has always been a concern with Americans, and undoubtedly will be so with regulation and legislation of individual private cyberspace users.

In all fairness to government, industry, and individual users alike, the rapid growth of information technology and their inability to keep up is another reason cyberspace is still unsecured. This is mostly due to practical financial reasons. Even if one were to outfit himself with the latest IT security hardware and software, these would be regarded as relatively obsolete within one-and-a-half to two years.[52] This means businesses, or anyone for that matter, must upgrade continuously to stay current with technology.[53] This undoubtedly can be very expensive when scaled over government directorates and large corporations.[54] Not only is the rapid pace of technology depleting budgets, it is outrunning the ability of lawmakers and regulators to keep pace.

Even technology developers struggle to keep up the pace. A good example is Microsoft's Windows operating systems, the predominant operating system platform for cyberspace users.[55] With every generation of faster computers, competition among software developers like Microsoft is driven by market forces to put newer versions of their bestsellers on ever-faster platforms. Often, the result is software released before all the bugs are eliminated. Microsoft has been criticized as these flaws have been exploited by cyberattacks.[56] While Microsoft releases patches to correct these flaws, many users remain ignorant of the necessity to install the patches. Even local area network (LAN) and systems administrators fail to apply the necessary patches because they are often overwhelmed by the enormity of the task. At the bottom of this heap is the individual user. For the most part, individual users have not been held accountable for failing to maintain their computer with up-to-date security, whether on the job or at home. This may be the weak link of it all, and probably the most difficult to correct.

Despite the seeming omnipresence of computers in the world, cyberspace is still very much an abstract concept to most users. Many managers in both government and industry think of security as a technology problem.[57] Some believe that if they throw enough money at

the IT department, this will solve the problem. Two things are wrong with this thought; first, this is not just a technology issue, but mostly one of management. [58] Technology can help, but by itself is not the solution. Second, especially since the downturn in the American economy, even if a technological solution were available money has not been, nor have many corporations been willing to spend money on cyberdefense in tougher economic times [59]. After all, with clamoring stockholders, the bottom line is what is important to corporate America; and unfortunately; many companies think that they are not vulnerable to cyberattack. It is like buying insurance; how much does one need, and more importantly, how much can one afford?

Government is less of a concern in this arena. Yes, money and the amount to spend on cyberdefense are and should always be a concern. However, since between 80-90% of all cyberspace infrastructure is privately owned,[60] one could conclude that it is industry's major responsibility to secure cyberspace. While this percentage figure seems to indicate government's piece of the cyberspace pie is only 10-20%, this does not account for the amount of infrastructure leasing the government does from the private sector. So while the government may only have up to 20% of the total infrastructure outright, it depends greatly on contracting from industry for the rest of its needs. The point is that government and private network are so intertwined and interdependent that neither could function well if the physical or virtual architecture of cyberspace was successfully attacked…especially if a virtual attack accompanied a physical attack.[61] Therefore, neither can ignore the other, nor assume the problem away to the other.

THE WAY AHEAD

No simple, silver-bullet solutions exist to fix cybersecurity in America. It will take a lot of work…and a lot of money, both in government, and especially in the private sector; and most likely will cost the private individual user as well. Because of the complexity of cyberspace in general, the solution to securing it is just as complex. Money, politics, and personal liberties are all going to be of concern as we tighten security; and the politics of it will make for interesting debate. Nonetheless, what follows are three recommendations to improve America's cybersecurity.

Much as the Transportation Security Agency (TSA) was created out of necessity to better secure air travel, the U.S. should not wait to create a like agency for cyberspace after a successful but devastatingly similar attack in cyberspace, especially since a framework of trained and experienced professionals exists already for such an agency in the newly-formed U.S. CERT. Further, there has been talk of doing what was once unthinkable, creating a

separate government network (called GovNet[62]) to better isolate government from the dangers of public cyberspace.

The talk should cease. It is now time to establish a GovNet with one agency or organization to monitor and control it, and the U.S. CERT is a good place to begin. A way to initially pay for it, partially if not entirely, would be from cost savings of consolidating government IT defense organizations into one network command and control hierarchy. A number of these organizations exist throughout government now, but operate independently of one another inside the various agencies. Over time, all U.S. Government agencies would migrate from what are now essentially their own private networks to the GovNet. Initially, each agency, and its own network operations and security center (NOSC) and CERT capabilities (which many also operate) would continue to maintain these; but as efficiencies are gained the total number of NOSCs and CERTS[63] would decrease.[64] In the end, instead of a number of NOSC/CERTs serving separate agencies and their networks, what would evolve is one inter-agency NOSC/CERT (a U.S. NOSC/CERT) overseeing all U.S. Government cybersecurity. Subordinated to this would be a number of NOSC/CERTs in a regional approach both in and out of the U.S., much like DOD, which already has NOSC/CERTs per each geographically aligned combatant commander.[65]

These inter-agency NOSC/CERTs, under the lead of the DHS via the U.S. NOSC/CERT, and jointly manned and operated through inter-agency cooperation, must then have the authority to require all government agencies to comply with security requirements PRIOR to connection to GovNet. The U.S. NOSC/CERT would then monitor all GovNet owned connections to the Internet, as well as cyberattacks developing within the public domain, giving advice not only internally, but to the public as well. If threatened seriously enough, it could isolate GovNet from the Internet temporarily to either prevent or mitigate the threat from gaining entrance, or isolate itself to prevent an internally introduced threat from getting out into the public domain. The primary purpose of the U.S. NOSC/CERT would be to provide unity of command and effort within the government's IT community, something sorely lacking at this time.

It will not be easy, nor cheap, to make this happen. Neither was the establishment of the TSA, or DHS, for that matter. However, the time to start is now, before a major cyberattack disrupts the government, and at significantly more cost vis-à-vis 11 September 2001. Much has been done, especially since 2001; but there is much still to be accomplished. A single integrated GovNet managed and controlled both operationally and administratively by a U.S.

NOSC/CERT and its regional subordinates would do much to improve the defense needed, but also demonstrate to the American IT world that government is serious about securing itself.

Government must then compel industry to comply. It can start by re-writing the cyber strategy with industry and other private concerns involvement, but with the necessary "teeth" to ensure success. A key part of the new cyber strategy must include a timeline, with a deadline that all can work towards. If voluntary compliance in a reasonable timeline cannot happen in an agreeable manner, then the administration must introduce legislation into the Congress to force the issue.

While public and private engagement is a key component to the national cyberspace strategy, government cannot hope business interests will necessarily police themselves. While a market economy will police itself along economic lines, it assumes fair access to markets; and today that means via cyberspace. Legislation and regulation will be necessary to require all participants in cyberspace to take the minimum amount of security measures necessary and maintain them prior to connection to cyberspace, and most certainly after connection.

A further part of the solution is the integration of industry into the U.S. NOSC/CERT concept as a full partner, including manning and operational costs shared by both. As the current U.S. CERT is already a partnership between government and private entities, this idea should be expanded to all of industry as well. However, assuming industry does not cooperate fully, the U.S. NOSC/CERT must be empowered by the Congress to monitor commercial cyberspace to ensure compliance of basic security rules…after it has also declared American cyberspace as public domain, because of its present (and obvious future) necessity to the security interests and economy of the U.S., subject to the same regulation and licensing as is the broadcast spectrum. Then, further empowered by the Congress with the authority to regulate industries' connection to cyberspace, including internet service providers (ISP), the U.S. NOSC/CERT can ensure that all entities in the public domain of cyberspace meet basic security requirements before connection. Anyone failing to do so could be disconnected, much like the Federal Communications Commission could deny broadcasting authority to a radio or television station if they do not comply with federal laws or regulation as it applies to this industry. Again, there is no attempt here to understate the potential controversy or subsequent difficulty of implementing this recommendation. This would indeed be a true paradigm shift in cyberspace management, and many Internet libertarians will scream foul long and hard. However, the alternative leaves a potential unacceptable threat to national security.

Corporate America must also assume their responsibilities in securing American cyberspace; and it has to be all of industry, not just the high-tech companies. Every company

with a computer system connected to cyberspace must be a part of the solution, as any not participating could be an unsecured threat, and thus should be disallowed from participating. Industry, by default, has the major role, as they are the majority "stockholder" in cyberspace. Because they own 80-90% of the nation's infrastructure, there can be no denying who will have the most work to do, or who will spend the most money in the process. But with the U.S. economy as the engine for the world economy,[66] the real question is can they afford not to? The obvious answer is no. Just the billions of dollars spent annually in consequence management and recovery from cyberattacks ought to convince industry that preventing cyberattacks is in its best interest. Acting after a debilitating attack to finally get serious about cybersecurity is pointless, and ultimately detracts from industry's bottom line.

Finally, but potentially the most problematic, individual computer users must also be held accountable. The days of absolute free and open access to the Internet may be at an end. When anyone can buy a high-end computer and gain broadband access to the Internet, failure to secure a computer can enable it to be used to launch attacks against others. The analogy of the early days of automobiles and airplanes when traffic was not a serious safety concern comes to mind. Today the U.S. has over 38,000 traffic fatalities annually[67]; and after September 11, who can doubt the seriousness of controlling where and how airplanes fly? Considering the strategic importance of cyberspace to the economy, governmental processes, and now to the American way of life, the U.S. cannot allow individual operators to continue to navigate through cyberspace in anonymous bliss, and certainly not with anonymous ill intent. Just as drivers of automobiles and pilots of airplanes are licensed, it is now time to license cyberspace surfers. Assuming a totally benign and altruistic cyber world, this would not be required. However, the ever-increasing technical sophistication of cyberspace, and more importantly the increasing erudition of the cyberattacker, now demands that one should know who is operating in cyberspace, while still maintaining the same privacy rules one may expect when driving one's personal automobile.

The licensing of individual employees on the job would be done by their employers, who in turn are licensed to access the public cyberspace domain by the U.S. NOSC/CERT. Employers would be held responsible for not just training and certifying their workers, but for their employees' bad behavior in cyberspace, just as corporations are held accountable for workers who are extremely negligent in their duties in other areas, such as when a worker driving the company delivery van commits some traffic violation leading to the damage of property or injury to other individuals. If nothing else, it would be just a matter of time until lawyers would begin to specialize in this type of cyber tort law.

With private cyberspace users, the task of licensing would go to ISPs. Three measures are necessary to make this happen: first, the anonymity of cyberspace users must cease. Individuals in anonymity tend to be bolder than when they are personally identified. While there is merit to requiring people to navigate through cyberspace using a user identification containing their realname@domain, each user should instead be issued an electronic signature from the ISP. [68] Not only will this deter anonymous surfers, in many instances electronic signatures have already been accepted legally as the electronic equivalent of the hand signature.[69] This allows use of an electronic signature to identify people when necessary, but would still allow them to use the user identification of their choice, allowing some privacy like that conveniently desired in chat rooms, or simply surf the net without fear of identity harvesting by cyberspace defrauders. Only the ISP would be able to identify the individual, and then only via proper legal request such as a search warrant, much the same way a bank safeguards an account holder's private information and number.

Next, ISPs would issue an online test of security procedures, rules, and laws that a new user must pass prior to issue of the license to the individual. Once a passing grade is achieved, the individual, for a fee of course, would be issued a license which includes the digital signature, the ISPs software download of mandatory, industry-produced, U.S. NOSC/CERT-approved firewall, anti-virus software, and other security software as the ISP and possibly the U.S. NOSC/CERT require, with mandatory automatic updates of this software by the ISP for the time the license is valid. This measure alone would probably greatly reduce the number of successful cyberattacks in cyberspace.

Once again, there is no attempt to understate the controversy and difficulty of this proposed recommendation. The process of licensing individuals for access to cyberspace will be fraught with many challenges, not the least of which will be criticism of encroachment upon civil liberties. Additionally, it further changes the paradigm of the way business is conducted in cyberspace; but much was probably the same when highways and flyways were also so originally regulated. However, as government, industry and individuals become more and more dependent on cyberspace, security becomes proportionally as important. One thing is certain, though; the U.S. can no longer allow cyberspace to go as unregulated as it has been to date.

CONCLUSION

The original ARPANET[70] was intended for use by researchers and academicians to corroborate their scientific findings, and so the inventors of this predecessor to the Internet did not foresee nor expect that anyone would intentionally behave badly. But just as many

American pioneers moved west to find new opportunities, so did the associated criminal element move with them; and so it has been with the Internet, ARPANET's successor. Even today the Internet is in many ways much like the old west, and many countries in the world are debating who should govern it.[71] If cyberspace is the future of business, then as more and more business finds itself conducted in this newest medium, the rate of regulation of cyberspace will probably increase proportionately.

The U.S. as a whole is still not doing enough to secure and defend cyberspace.[72] The strategic implications of this should be clear; all sectors of American society are now dependent upon cyberspace, and this dependency grows rapidly daily. Until now cyberspace has existed with relatively unregulated access. However, as the reliance on cyberspace grows, the subsequent requirement for security also grows with it. We must now take at least the minimum necessary measures to better secure cyberspace, or continue to suffer the consequences of computer attacks from a variety of threats. The U.S. Government must first set the example by securing itself, and then move to bring industry into compliance, preferably through consensus, but if necessary through regulation or legislation. While government should display the necessary leadership in this arena, industry has the great majority of the nation's infrastructure, and therefore will bear the largest burden. Finally, individual users must take a more active role in securing their small part of cyberspace. The recommendations contained herein may not be the final solution, and most likely will be controversial. Nonetheless, they provide at the very least a point of departure from which to continue the debate on securing American cyberspace in order to prevent the potential digital Pearl Harbor or electronic September 11 from ever occurring.

WORD COUNT=5909

ENDNOTES

[1] Dan Verton, "Interview: Outflanking the Cyberterrorist Threat," *CNN.com* 11 April 2002 [journal on-line]; available from http://www.cnn.com/2002/TECH/industry/04/11/interview.cybersecurity.idg/; Internet; accessed 22 September 2003.

[2] Internet.com, Webopedia, (Darien, CT: Jupitermedia Corporation, 2004); available from http://www.webopedia.com/TERM/v/virus.html; Internet; accessed 15 February 2004. According to Webopedia, *cyberspace is* a metaphor for describing the non-physical terrain created by computer systems. Online systems, for example, create a cyberspace within which people can communicate with one another (via e-mail), do research, or simply window shop. Like physical space, cyberspace contains *objects* (files, mail messages, graphics, etc.) and different modes of transportation and delivery. Unlike real space, though, exploring cyberspace does not require any physical movement other than pressing keys on a keyboard or moving a mouse. Some programs, particularly computer games, are designed to create a special cyberspace, one that resembles physical reality in some ways but defies it in others. In its extreme form, called *virtual reality*, users are presented with visual, auditory, and even tactile feedback that makes cyberspace feel real. The term was coined by author William Gibson in his sci-fi novel Neuromancer (1984).

[3] Robert Lemos, "Counting the Cost of Slammer," *CNET News.com* 31 January 2003 [journal on-line]; available from http://news.com.com/2102-1001_3-982955.html?tag=st_util_print; Internet; accessed 26 January 2004. This article by Lemos reports that in one instance alone, the Slammer worm, which hit networks in late February 2003, caused between $950 million and $1.2 billion. At its height, Slammer denied access to the Internet of several U.S. Army installations in the continental U.S.

[4] Internet.com, Webopedia, (Darien, CT: Jupitermedia Corporation, 2004); available from http://www.webopedia.com/TERM/v/virus.html; Internet; accessed 27 January. According to Webopedia, a virus is defined as, "A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are manmade. A simple virus that can make a copy of itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems."

[5] Jonathan Krim, "Help Fix Cyber-Security Or Else, U.S. Tells Industry," *Washingtonpost.com*, 4 December 2003 [journal on-line], available from http://www.washingtonpost.com/wp-dyn/articles/A33245-2003Dec3.html; Internet; accessed 4 December 2003. This article reports that a number of worms and viruses in late summer 2003 caused the U.S. $3.5 billion in damages due to lost time (access to systems) and consequence management to restore services to users.

[6] The Terrorism Research Center, Inc., website definition of cyberterror attributed to the FBI, 6 December 2003, available from http://www.terrorism.com/modules.php?op=modload&name=News&file=article&sid=10145; Internet; accessed 6 December 2003.

[7] The London Free Press, "Cyber Attacks a Concern," Overseas Advisory Council, 25 April 2003; available from http://www.ds-osac.org/view.cfm?key=7E4451414757&type=2B170C1E0A3A0F162820; Internet; accessed 6 December 2003.

[8] Robert H. Allen, "Asymmetric Warfare: Is the Army Ready?" Student Paper, Army Management Staff College Online, Publications, Student Articles, 1997; available from http://www.amsc.belvoir.army.mil/asymmetric_warfare.htm ; Internet; accessed 6 December 2003.

[9] So much so that the Department of Homeland Security entered into a partnership with Carnegie Mellon's CERT to form the U.S. CERT. See Jonathan Krim, "Help Fix Cyber-Security Or Else, U.S. Tells Industry," *Washingtonpost.com* , 4 December 2003 [journal on-line], available from http://www.washingtonpost.com/wp-dyn/articles/A33245-2003Dec3.html; Internet; accessed 4 December 2003.

[10] Carnegie Mellon Software Engineering Institute, CERT Coordination Center Statistics 26 January 2004; available from http://www.cert.org/stats/cert_stats.html; Internet; accessed 26 January 2004. It is very likely that these numbers are much lower than the actual count, as many attacks have not been recognized as attacks, and many attacks are likely not reported.

[11] According to Jonathon Krim of the *Washington Post*, he reports that the CERT Coordination Center states cyberattacks were up 40% in the first three quarters of 2003. See his article, "Help Fix Cyber-Security of Else, U.S. Tells Industry," *Washingtonpost.com* , 4 December 2003.

[12] Matthew French, "DOD: Systems Need More Protection," *Federal Computer Weekly* 28 July 2003 [journal on-line]; available from http://www.fcw.com/fcw/articles/2003/0728/web-DoD-07-28-03.asp; Internet; accessed 26 January 2004.

[13] Suzanne Gaspar, "Securing Your share or Cyberspace," *NetworkWorldFusion* 18 October 2002; [journal on-line]; available from http://www.nwfusion.com/news/2002/1018 clarkecybersec.html; Internet; accessed 26 January 2003.

[14] Jonathan Krim, "Help Fix Cyber-Security Or Else, U.S. Tells Industry," *Washingtonpost.com* 4 December 2003 [journal on-line]; available from http://www.washingtonpost.com/wp-dyn/articles/A33245-2003Dec3.html, Internet; accessed 26 January 2004. Krim states here that the private sector owns "roughly 85% of the country's computer infrastructure." Dan Verton states the same in his article, "Former CIA Chief Sees Need for Greater Network Resilience, Market Incentives," *Computerworld* 29 October 2003; [journal on-line]; available from http://www.computerworld.com/industrytopics/energy/story/ 0,10801,86638,00.html; Internet; accessed 26 January 2004. A *San Jose Mercury News* editorial on 3 December 2003 states, "With about 90% of the electronic infrastructure in private hands…." "Tech Security Has a Weak Link," The *San Jose Mercury News* 3 December 2003 [journal on-line]; available from http://nl.newsbank.com/nl-search/we/Archives?s_site= mercurynews&p_multi=SJ|&p_product=SJ&p_theme=realcities&p_action=search&p_maxdocs= 200&p_text_search-0=Tech%20AND%20security%20AND%20has%20AND%20a%20 AND%20weak%20AND%20link&s_dispstring=Tech%20security%20has%20a%20weak%20link %20AND%20date(last%20180%20days)&p_field_date-0=YMD_date&p_params_date-0=date:B,E&p_text_date-0=-180qzD&p_perpage=10&p_ sort=YMD_date:D&xcal_ useweights=no; Internet; accessed 3 December 2004.

[15] This is an extrapolated estimate for the sake of continuing the argument on the amount of IT security spent.

[16] Jonathan Krim, "Help Fix Cyber-Security Or Else, U.S. Tells Industry", *Washingtonpost.com* 4 December 2003 [journal on-line]; available from http://www.washingtonpost.com/wp-dyn/articles/A33245-2003Dec3.html, Internet; accessed 26 January 2004. Also, see Alison Diana "Does the Killer Worm Really Exist?" E-Commerce Times, 14 September 2003 [journal on-line]; available from http://www.ecommercetimes.com/perl/story/31550.html; Internet; accessed 27 January 2004.

[17] Computer Associates, Virus Information Center; Glossary of Terms, (Computer Associates International, Inc., 2004); available from http://www3.ca.com/virusinfo/glossary.aspx#W; Internet; accessed 27 January 2004. According to *Glossary of Terms*, "In the Wild; a term that indicates a virus has been found infecting systems in several organizations around the world. Ideally, the term is reserved for viruses that currently are (or, that have been) in the 'top half' of the WildList. This contrasts the virus with those that have only been reported by antivirus researchers, and which are sometimes referred to as 'zoo viruses' or 'collection viruses.' Despite popular hype, most viruses are not 'in the wild' and are unlikely ever to be."

[18] Internet.com, Webopedia, (Darien, CT: Jupitermedia Corporation, 2003); available from http://www.webopedia.com/TERM/D/DoS_attack.html; Internet; accessed 27 January 2004. According to Webopedia, "DoS; short for denial-of-service attack, a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCP/IP protocols. For all known DoS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks. But, like viruses, new DoS attacks are constantly being dreamed up by hackers. Also see Elizabeth G. Book, "Info-Tech Industry Targets Diverse Threats," *National Defense Magazine*, August 2002 [journal on-line]; available from http://www.nationaldefensemagazine.org/article.cfm?Id=876; Internet; accessed 27 January 2004.

[19] Robert Lemos, "Counting the Cost of Slammer," *CNET News.com* 31 January 2003 [journal on-line]; available from http://news.com.com/2100-1001-982955.html; Internet, accessed 27 January 2004.

[20] Ibid.

[21] Elise Ackerman, "Computer Security in Focus," *SiliconValley.com* 3 December 2003 [journal on-line]' available from http://www.siliconvalley.com/mld/siliconvalley/7402121.htm?template=contentModules/printstory.jsp; Internet; accessed 27 January 2004.

[22] Ibid.

[23] Brian Krebs, "Cybersecurity Draft Plan Soft on Business, Observers Say," *Washingtonpost.com* 19 September 2002 [journal on-line]; available from http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A35812-2002Sep18&notFound=true; Internet; accessed 3 December 2003.

[24] Mitre Corporation, "What is the Y2K Problem?" 27 January 1999; available from http://www.mitre.org/tech/y2k/docs/PROB.html; Internet; accessed 27 January 2004. "Briefly defined, the Y2K problem involves any or all of these: Representing the year as a two-digit number, causing failures in arithmetic, comparisons, sorting, and input/output to databases or files when manipulating date data: incorrect software will assume that the maximum value of a

year field is '99' and will roll systems over to '00' which can be mistakenly interpreted as 1900 rather than 2000, resulting in negative date calculations and the creation of many overnight centenarians. Incorrect leap year calculations will assume that the year 2000 has only 365 days instead of 366. What's more, although January 1, 2000 is the primary witching hour, many date-dependent algorithms and forward-referencing systems are already beginning to fail due to not properly classifying years divisible by 400; and Software values involving limited date ranges, including hard-coded values and "magic bullets" limits to system date data types in hardware registers."

[25] Having the hard Y2K timeline of 1 January 2000 provided all with a hard and fast timeline. Y2K was going to happen with or without government, industry or individual input. Maybe what is required here is a hard date to implement security measures needed. Assuming these measures could be agreed upon, the challenge lies in who would be responsible to monitor and then enforce it all, not to mention who pays. It will probably take government regulation or legislation to make it happen unless industry and government can agree.

[26] Brian Krebs, "Cybersecurity Draft Plan Soft on Business, Observers Say," *Washingtonpost.com* 19 September 2002 [journal on-line]; available from http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A35812-2002Sep18&notFound=true; Internet; accessed 3 December 2003.

[27] Having a fixed date of 1 January 2000 undoubtedly helped this process greatly. Not knowing exactly when a large cyberattack will happen does not ease the movement towards cybersecurity. Also, there are still many who question whether a debilitating cyberattack could occur further hinders the process. However, one should also ask whether anyone thought flying hijacked airliners into buildings causing the destruction and chaos they did, was possible prior to 11 September 2001. Therefore, a hard date for fixing the identified strategic weaknesses of American cyberspace should be discussed, assuming the worst-case scenario, or at least the most-probable case scenario, towards which government, industry and individuals can work.

[28] Robert Lemos, "Counting the Cost of Slammer," *CNET News.com* 31 January 2003 [journal on-line]; available from http://news.com.com/2102-1001_3-982955.html?tag=st_util_print; Internet; accessed 26 January 2004.

[29] Bruce Schneier, "Internet Worms and Critical Infrastructure," *CNET News.com* 9 December 2003 [journal on-line]; available from http://news.com.com/2010-7343_3-5117862.html; Internet; accessed 27 January 2004.

[30] Robert Lemos, "Cybersecurity Task Forces Push for Results," *CNET News.com* 4 December 2003 [journal on-line]; available from http://news.com.com/2100-7348-5113630.html; Internet; accessed 27 January 2004

[31] Brian Krebs, "Cybersecurity Draft Plan Soft on Business, Observers Say," *Washingtonpost.com* 19 September, 2002 [journal on-line]; available from http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A35812-2002Sep18&notFound=true; Internet; accessed 27 January 2004.

[32] Ibid.

[33] Ibid.

[34] Industry has been fighting efforts on a global scale as countries within the U.N. have complained about ICANN's (Internet Corporation for Assigned Names and Numbers) control of the Internet), amongst many issues, but taxes being one of them. See Wong Choon Mei, "Fight Looms over Control of Internet," *Yahoo! News Technology – Reuters* Internet Report 16 September 2003 [journal on-line]; available from http://in.tech.yahoo.com /030916/137/27t9d.html; Internet; accessed 27 January 2004. ICANN is an internationally organized, non-profit corporation that has responsibility for Internet Protocol (IP) address space allocation, protocol identifier assignment, generic (gTLD) and country code (ccTLD) Top-Level Domain name system management, and root server system management functions. These services were originally performed under U.S. Government contract by the Internet Assigned Numbers Authority (IANA) and other entities. ICANN now performs the IANA function. As a private-public partnership, ICANN is dedicated to preserving the operational stability of the Internet; to promoting competition; to achieving broad representation of global Internet communities; and to developing policy appropriate to its mission through bottom-up, consensus-based processes. For more details on ICANN, see ICANN, "What is ICANN?" 13 January 2004, [journal on-line]; available from http://www.icann.org/general/; Internet; accessed 31 January 2004.

[35] Associated Press, "Tech Companies Oppose Government Security Rules," *BizReport* 3 December 2003 [journal on-line]; available from http://www.bizreport.com/article.php?art_ id=5668&PHPSESSID=c33a20e536f6acb6c290fd0d354efe8d; Internet; accessed 27 January 2004.

[36] Cynthia L. Webb, "Cybersecurity Talk is Cheap," *Washingtonpost.com* 3 December 2003 [journal on-line]; available from http://www.washingtonpost.com/ac2/wp-dyn/A31089-2003Dec3?language=printer; Internet; accessed 3 December 2003.

[37] Andy Sullivan, "U.S. Homeland Chief Urges SEC Cybersecurity Filings," *Reuters* via *USA Today Tech* 9 October 2003 [journal on-line]; available from http://www.usatoday.com/ tech/news/computersecurity/2003-10-09-sec-cyberfiling-idea_x.htm; Internet; accessed 27 January 2004.

[38] Jonathan Krim, "Help Fix Cyber-Security Or Else, U.S. Tells Industry," *Washingtonpost.com* 4 December 2003 [journal on-line], available from http://www.washingtonpost.com/wp-dyn/articles/A33245-2003Dec3.html, accessed 4 December 2003.

[39] David Becker and Matt Hines, "FBI Arrests MSBlast Worm Suspect," *CNET News.com* 29 August 2003 [journal on-line]; available from http://news.com.com/2100-1009-5070000.html; Internet; accessed 27 January 2004.

[40] Carrie Kirby, "Internet Security Gets Checkup: Tech Leaders, Feds Take New Look at Plan," *SFGate.com* 3 December 2003 [journal on-line); available from http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2003/12/03/BUG903EG9S1. DTL&type=business; Internet; accessed 27 January 2004.

[41] Robert Lemos, "Tech Industry Put on Security Notice," *CNET News.com* 3 December 2003 [journal on-line]; available from http://news.com.com/2100-7355-5113165.html; Internet; accessed 27 January 2004.

[42] Ibid.

[43] Ibid.

[44] Ibid.

[45] Charles Cooper, "Copping Out on Cybersecurity," *CNET News.com* 5 December 2003 [journal on-line]; available from http://news.com.com/2009-7348-5113645.html; Internet; accessed 27 January 2004.

[46] Five working groups were formed at the National Cyber Security Summit in December 2003 with a focus on delivering results within a year. For more info see Robert Lemos, "Cybersecurity Task Forces Push for Results," *CNET News.com* 4 December 2003 [journal on-line]; available from http://news.com.com/2100-7348-5113630.html; Internet; accessed 27 January 2004.

[47] Mercury News Editorial, "Tech Security Has a Weak Link," *The San Jose Mercury News* 3 December 2003 [journal on-line]; available from http://nl.newsbank.com/nl-search/we/Archives?s_site=mercurynews&p_multi=SJ|&p_product=SJ&p_theme=realcities&p_action=search&p_maxdocs=200&p_text_search-0=Tech%20AND%20security%20AND%20has%20AND%20a%20%20AND%20weak%20AND%20link&s_dispstring=Tech%20security%20has%20a%20weak%20link%20AND%20date(last%20180%20days)&p_field_date-0=YMD_date&p_params_date-0=date:B,E&p_text_date-0=-180qzD&p_perpage=10&p_%20sort=YMD_date:D&xcal_useweights=no; Internet; accessed 3 December 2004.

[48] At the conclusion of writing this paper, the deadline of 1 March 2004 had not been reached, and so the planned-for outcomes could not be reviewed and their results possibly considered.

[49] Intel produced the 8086 prior to the 8088, and it was actually a better processor, but too expensive for PC use.

[50] Internet.com, Webopedia, (Darien, CT: Jupitermedia Corporation, 2003); available from http://www.webopedia.com ; Internet; accessed 18 October 2003. According to Webopedia, "A Zombie computer that has been implanted with a daemon that puts it under the control of a malicious hacker without the knowledge of the computer owner. Zombies are used by malicious hackers to launch DoS attacks . The hacker sends commands to the zombie through an open port. On command, the zombie computer sends an enormous amount of packets of useless information to a targeted Web site in order to clog the site's routers and keep legitimate users from gaining access to the site. The traffic sent to the Web site is confusing and therefore the computer receiving the data spends time and resources trying to understand the influx of data that has been transmitted by the zombies. Compared to programs such as viruses or worms that can eradicate or steal information, zombies are relatively benign as they temporarily cripple Web sites by flooding them with information and do not compromise the site's data. Such prominent sites as Yahoo!, Amazon and CNN.com were brought down in 2000 by zombie DoS attacks."

[51] See Denial of Service Attack at endnote 18 above.

[52] One reason for this is Moore's Law. Named after Gordon Moore, co-founder of Intel, Moore's law states computing power doubles approximately every eighteen to twenty-four months. By itself, Moore's Law does not cause this obsolescence directly, but rather indirectly as the increase in computing power competitively drives both hardware and software manufacturers to develop peripheral computer capabilities capable of keeping up with the newly developed PC chip power that Moore's Law postulates. See Internet.com, Webopedia, (Darien, CT: Jupitermedia Corporation, 2004); available from http://www.webopedia.com ; Internet; accessed 18 October 2003. According to Webopedia, the observation made in 1965 by Gordon Moore, co-founder of Intel, that the number of transistors per square inch on integrated circuits had doubled every year since the integrated circuit was invented. Moore predicted that this trend would continue for the foreseeable future. In subsequent years, the pace slowed down a bit, but data density has doubled approximately every 18 months, and this is the current definition of Moore's Law, which Moore himself has blessed. Most experts, including Moore himself, expect Moore's Law to hold for at least another two decades.

[53] Moore's Law supports this. See endnote above. However, also see Michael Kanelleos, "Moore says Moore's Law to Hit Wall," *CNET News.com* 30 September 2004 [journal on-line]; available from http://news.com.com/2010-7343_3-5117862.html; Internet; accessed 27 January 2004. This discusses that Moore's Law may cease to be a factor around the year 2020, plus or minus 2-3 years.

[54] The one positive trend here is that, generally speaking, technology costs have been coming down as IT proliferates.

[55] It can be argued that Microsoft's Windows operating systems have been highly successful simply due to their dominance in the market. However, this means that when a vulnerability is discovered, or worse exploited, the majority of cyberspace users can be affected. While Windows may be have become a de facto operating system throughout most of the personal computing world, the fact is this makes the majority of users vulnerable because of not incorporating back up operating systems and back up software to run on top of it. Criticism against this potential over-reliance on one operating system seems to be growing as of this writing.

[56] Kevin Krolicki and Reed Stevenson, "Microsoft Faces Class Action over Virus Crashes," *Yahoo! News* 2 October 2003 [journal on-line]; available from http://www.biz.yahoo.com/rc/031002/tech_microsoft_security_3.html; Internet; accessed online 5 October 2003.

[57] Michael Rasmussen, "The Cybersecurity Challenge," *Washingtonpost.com* 5 December 2003 [journal on-line]; available from http://www.washingtonpost.com/ac2/wp-dyn/A35977-2003Dec4?language=printer; Internet; accessed 27 January 2004.

[58] Ibid.

[59] Rachel Konrad, "Homeland Security Chief Warns Tech Firms to Cooperate on Cybercrime," *Seattletimes.com* 4 December 2003 [journal on-line]; available from http://archives.seattletimes.nwsource.com/cgi-in/texis.cgi/web/vortex/display?slug= compsecure04&date= 20031204; Internet; accessed 4 December 2003.

[60] Jonathan Krim, "Help Fix Cyber-Security Or Else, U.S. Tells Industry," *Washingtonpost.com* 4 December 2003 [journal on-line]; available from http://www.washingtonpost.com/wp-dyn/articles/A33245-2003Dec3.html; Internet; accessed 4 December 2003.

[61] Jonathan Adams and Fred Guterl, "Bringing down the Internet," *MSNBC News Newsweek* 3 November 2003 [journal on-line]; available from http://msnbc.msn.com/id/3339638/; Internet; accessed 27 January 2004.

[62] William New, "Demand Grows for Government only network," *Government Executive Magazine*, 29 January 2004; [journal on-line]; available from http://www.govexec.com/homeland/; Internet; accessed 5 February 2004.

[63] Often, though these two organizations, NOSC and CERT, are operated by independent organizations, they are many times physically located and operate together in complementary fashion. Such an example is the U.S. Army's Continental United States – Theater Network Operations and Security Center (CONUS TNOSC) operated by the U.S. Army Network Enterprise and Technology Command (USANETCOM), and the Regional Computer Emergency Response Team – CONUS (RCERT-C), operated by the U.S. Army 1st Information Operations Command. The CONUS – TNOSC/RCERT- C is located at Fort Huachuca, AZ. You can view their joint website at http://www.conus-tnosc.army.mil/jointentry/; Internet; accessed 16 February 2004. Another great example of this is the U.S. Army NOSC (ANOSC) and the U.S. Army CERT (ACERT) jointly located at Fort Belvoir, Virginia; see https://www.acert.belvoir.army.mil/.

[64] For example, DOD has its own CERT and Network Operations and Security Centers, as do each of the services and many subordinate, like organizations throughout the world dedicated to monitoring and defending the military's portion of cyberspace. DOD, via DISA, operates the Global Network Operations and Security Center (GNOSC), located in Arlington, Virginia, and has regional subordinate organizations, call Regional Network Operations and Security Centers (RNOSC) assigned to each Combatant Commander under the DOD regional construct.

[65] It is not important whether it is a DOD combatant command's regional construct, or some other, say that of the State Department's. What is more important is a regional, inter-agency approach led by the U.S. NOSC/CERT that is being proposed here, under the direction of DHS for the purpose of unity of command/control and unity of effort. DOD is suggested as an example, as they already have such functions ongoing within each of its regions (RNOSCs) under the auspices of the Defense Information Systems Agency (DISA), and its GNOSC.

[66] Suzanne Gaspar, "Securing Your share or Cyberspace," *NetworkWorldFusion* 18 October 2002; [journal on-line]; available from http://www.nwfusion.com/news/2002/1018clarkecybersec.html; Internet; accessed 26 January 2003.

[67] National Center for Statistics & Analyses, "Fatality Analysis Reporting System (FARS) Web-Based Encyclopedia," National Highway and Traffic Safety Agency 2004; available from http://www-fars.nhtsa.dot.gov/; Internet; accessed 6 February 2004. This site reports in 2002 there were 38,309 motor vehicle fatalities.

[68] This is not a new concept. Martin Libicki, in his 1995 essay, "What is Information Warfare?" suggested "digital signatures" as a defense against "cyberwarfare." See Martin Libicki, "What is information Warfare?" August 1995; available from http://www.iwar.org.uk/iwar/resources/ndu/infowar/a003cont.html; Internet; accessed 8 February 2004. The Department of Defense, in 2001, began issuing new identification cards to all of its employees, including contractor personnel, called the Command Access Card, or CAC card for short. The card is the size of a standard credit card. Besides being an official photo ID, it contains, among many things, a personal digital signature, personal identification number (PIN) code, and a biometric (digitized thumbprint). However, as of early 2004, the CAC cards are not in wide use yet outside of Washington, DC. Besides this, the electronic or digital signature has not yet made its way out to the U.S. en masse, and it is suggested here that it would go a long way to helping secure cyberspace, especially at the individual user level.

[69] There are a number of websites about electronic (e-signature) or digital signatures available. Some show where it has been codified into law, such as Title 21 Code of Federal Regulations (21 CFR Part 11), Electronic Records; Electronic Signatures, at the Federal Drug Administration's website; Internet; available from http://www.fda.gov/ora/compliance_ref/part11/, accessed 8 February 2004. Another is the commercial website by Rogers, Joseph, O'Donnell & Phillips, Attorney's at Law, available from http://www.rjop.com/publish45.htm#intro; Internet; accessed 8 February 2003. Many more can be found by entering "digital signature" in any of the popular Internet search engines.

[70] Internet.com, Webopedia, (Darien, CT: Jupitermedia Corporation, 2004); available from http://www.webopedia.com/TERM/A/ARPANET.html; Internet; accessed 27 January 2004. According to Webopedia, "The precursor to the Internet, ARPANET was a large wide-area network created by the United States Defense Advanced Research Project Agency (ARPA). Established in 1969, ARPANET served as a test bed for new networking technologies, linking many universities and research centers. The first two nodes that formed the ARPANET were UCLA and the Stanford Research Institute, followed shortly thereafter by the University of Utah."

[71] Wong Choon Mei, "Fight Looms over Control of Internet," *Yahoo! News Technology – Reuters Internet Report* 16 September 2003 [journal on-line]; available from http://in.tech.yahoo.com /030916/137/27t9d.html; Internet; accessed 27 January 2004.

[72] Even as this paper is being finalized late in February 2004, the Congress pressed DHS on cybersecurity in the U.S. Government. *Yahoo! News.com* reported on 24 February 2004 that Jonathon Krim of the *Washington Post* wrote; "Sen. Jon Kyl (R-Ariz.) expressed surprise and frustration when a Department of Homeland Security official testified that his agency has not compiled a comprehensive analysis of vulnerabilities to cyber-attacks. Kyl said the number of security intrusions reported to the Internet security coordination center at Carnegie Mellon rose from 84,000 in 2002 to 137,000 in 2003, some causing millions of dollars in damages. Amit Yoran, who heads the department's cyber-security division formed last year, said the Department of Homeland Security takes an integrated approach to all terrorist threats and does not look at computer vulnerabilities in isolation. Asked by Sen. Dianne Feinstein (D-Calif.) whether his department has issued any directives to other federal agencies about improving security, Yoran responded that he works closely with them. 'I take it the answer is no,' said Feinstein, the only other senator to appear at the hearing of the Judiciary subcommittee on terrorism, technology and homeland security, which Kyl heads. For the full article see Jonathon Krim, "Cyber-Security Coordination Lacking, Senators Contend," *Yahoo! News Technology – washingtonpost.com* , 24 February 2004 [journal on-line]; available from

http://story.news.yahoo.com/news?tmpl=story&u=/washpost/20040225/tc_washpost/a3314_2004feb24; Internet; accessed 26 February 2004.

GLOSSARY

ARPA	Advanced Projects Research Agency
ARPANET	Advance Research Projects Agency Network
CAC	Common Access Card
ccTLD	country code Top-Level Domain
CERT	Computer Emergency Response Team
CND	Compute r Network Defense
CNO	Computer Network Operations
CONUS	Continental United States
DHA	Department of Homeland Security
DISA	Defense Information Systems Agency
DOD	Department of Defense
DoS	Denial of Service
FARS	Fatality Analysis Reporting System
GNOSC	Global Network Operations and Security Center
GovNet	Government Network
gTLD	generic Top-Level Domain
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ISP	Internet Service Provide
IT	Information Technology
NOSC	Network Operations and Security Center
RCERT	Regional Computer Emergency Reaction Team
RNOSC	Regional Network Operations and Security Center
TNOSC	Theater Network Operations and Security Center
TSA	Transportation Security Administration
U.S.	United States
USA	United States Army
USACERT	U.S. Army Computer Emergency Response Team
USANETCOM	U.S. Army Network Enterprise & Technology Command
USAWC	U.S. Army War College

BIBLIOGRAPHY

Ackerman, Elise. "Computer Security in Focus." *SiliconValley.com* 3 December 2003. Journal on-line. Available from http://www.siliconvalley.com/mld/siliconvalley/7402121.htm?template=contentModules/printstory.jsp. Internet. Accessed 27 January 2004.

Adams, Jonathan and Fred Guterl. "Bringing down the Internet." *MSNBC News Newsweek* 3 November 2003. Journal on-line. Available from http://msnbc.msn.com/id/3339638/. Internet. Accessed 27 January 2004.

Allen, Robert H. "Asymmetric Warfare: Is the Army Ready?" Army Management Staff College Online 1997. Available from http://www.amsc.belvoir.army.mil/asymmetric_warfare.htm. Internet. Accessed 6 December 2003.

Associated Press. "Tech Companies Oppose Government Security Rules." *BizReport* 3 December 2003. Journal on-line. Available from http://www.bizreport.com/article.php?art_id=5668&PHPSESSID=c33a20e536f6acb6c290fd0d354efe8d. Internet. Accessed 27 January 2004.

Becker, David and Matt Hines. "FBI Arrests MSBlast Worm Suspect." *CNET News.com* 29 August 2003. Journal on-line. Available from http://news.com.com/2100-1009-5070000.html. Internet. Accessed 27 January 2004.

Carnegie Mellon Software Engineering Institute. "CERT Coordination Center Statistics." 26 January 2004. Available from http://www.cert.org/stats/cert_stats.html. Internet. Accessed 26 January 2004.

Computer Associates International, Inc. "Glossary of Terms." Virus Information Center 2004.Available from http://www3.ca.com/virusinfo/glossary.aspx#W. Internet. Accessed 27 January 2004.

Cooper, Charles. "Copping Out on Cybersecurity." *CNET News.com* . 5 December 2003. Journal on-line. Available from http://news.com.com/2009-7348-5113645.html. Internet. Accessed 27 January 2004.

Electronic Records; Electronic Signatures. Title 21 Code of Federal Regulations (21 CFR Part 11). Federal Drug Administration March 2000. Internet. Available from http://www.fda.gov/ora/compliance_ref/part11/, accessed 8 February 2004.

French, Matthew. "DoD: Systems Need More Protection." *Federal Computer Weekly* 28 July 2003. Journal on-line. Available from http://www.fcw.com/fcw/articles/2003/0728/web-DoD-07-28-03.asp. Internet. Accessed 26 January 2004.

Gaspar, Suzanne. "Securing Your Share of Cyberspace." *NetworkWorldFusion* 18 October 2002. Journal on-line. Available from http://www.nwfusion.com/news/2002/1018clarkecybersec.html. Internet. Accessed 26 January 2003.

Internet Corporation for Assigned Names and Numbers (ICANN). "What is ICANN?" ICANN 13 January 2004. Available from http://www.icann.org/general/. Internet. Accessed 31 January 2004.

Internet.com. Webopedia (Darien, CT: Jupitermedia Corporation, 2003) 24 November 2003. Available from http://www.webopedia.com. Internet. Accessed 27 January 2004.

Kanelleos, Michael. "Moore says Moore's Law to Hit Wall." *CNET News.com* 30 September 2004. Journal on-line. Available from http://news.com.com/2010-7343_3-5117862.html. Internet. Accessed 27 January 2004.

Kirby, Carrie. "Internet Security Gets Checkup: Tech Leaders, Feds Take New Look at Plan." *SFGate.com* 3 December 2003. Journal on-line. Available from http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2003/12/03/BUG903EG9S1.DTL&type=business. Internet. Accessed 27 January 2004.

Konrad, Rachel. "Homeland Security Chief Warns Tech Firms to Cooperate on Cybercrime." *Seattletimes.com* 4 December 2003. Journal on-line. Available from http://archives.seattletimes.nwsource.com/cgi-in/texis.cgi/web/vortex/display?slug=compsecure04&date=20031204. Internet. Accessed 4 December 2003.

Krebs, Brian. "Cybersecurity Draft Plan Soft on Business, Observers Say." *Washingtonpost.com* 19 September 2002. Journal on-line. Available from http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A35812-2002Sep18&notFound=true. Internet. Accessed 3 December 2003.

Krim, Jonathon. "Cyber-Security Coordination Lacking, Senators Contend." *Yahoo! News Technology – washingtonpost.com* 24 February 2004 [journal on-line]. Available from http://story.news.yahoo.com/news?tmpl=story&u=/washpost/20040225/tc_washpost/a3314_2004feb24. Internet. Accessed 26 February 2004.

Krim, Jonathan. "Help Fix Cyber-Security Or Else, U.S. Tells Industry." *Washingtonpost.com* 4 December 2003. Journal on-line. Available from http://www.washingtonpost.com/wp-dyn/articles/A33245-2003Dec3.html. Internet. Accessed 4 December 2003.

Krolicki, Kevin and Reed Stevenson. "Microsoft Faces Class Action over Virus Crashes." Yahoo! News 2 October 2003. Journal on-line. Available from http://www.biz.yahoo.com/rc/031002/tech_microsoft_security_3.html. Internet. Accessed online 5 October 2003.

Lemos, Robert. "Counting the Cost of Slammer." *CNET News.com* 31 January 2003. Journal on-line. Available from http://news.com.com/2102-1001_3-982955.html?tag=st_util_print. Internet. Accessed 26 January 2004.

Lemos, Robert. "Cybersecurity Task Forces Push for Results." *CNET News.com* 4 December 2003. Journal on-line. Available from http://news.com.com/2100-7348-5113630.html. Internet. Accessed 27 January 2004.

Lemos, Robert. "Tech Industry Put on Security Notice," *CNET News.com* 3 December 2003. Journal on-line. Available from http://news.com.com/2100-7355-5113165.html. Internet. Accessed 27 January 2004.

Libicki, Martin. "What is information Warfare?" August 1995. Available from http://www.iwar.org.uk/iwar/resources/ndu/infowar/a003cont.html. Internet. Accessed 8 February 2004.

London Free Press. "Cyber Attacks a Concern." Overseas Advisory Council 25 April 2003. Available from http://www.ds-osac.org/view.cfm?key=7E4451414757&type= 2B170C1E0A3A0F162820. Internet. Accessed 6 December 2003.

Mitre Corporation. "What is the Y2K Problem?" 27 January 1999. Available from http://www.mitre.org/tech/y2k/docs/PROB.html; Internet accessed 27 January 2004.

National Center for Statistics & Analyses. "Fatality Analysis Reporting System (FARS) Web Based Encyclopedia." National Highway Safety and Transportation Agency 13 February 2004. Available from http://www-fars.nhtsa.dot.gov/. Internet. Accessed 6 February 2004.

New, William. "Demand Grows for Government Only Network." Government Executive Magazine 29 January 2004. Journal on-line. Available from http://www.govexec.com /homeland/. Internet. Accessed 5 February 2004.

Rasmussen, Michael. "The Cybersecurity Challenge." *Washingtonpost.com* 5 December 2003. Journal on-line. Available from http://www.washingtonpost.com/ac2/wp-dyn/A35977-2003Dec4?language=printer. Internet. Accessed 27 January 2004.

Rogers, Joseph, O'Donnell & Phillips, Attorney's at Law. "Electronic Signatures Statutes." December 2002. Available from http://www.rjop.com /publish45.htm#intro. Internet. Accessed 8 February 2003.

San Jose Mercury News. "Tech Security Has a Weak Link." 3 December 2003. Journal on-line. Available from http://nl.newsbank.com/nl-search/we/Archives?s_site= mercurynews&p_multi=SJ|&p_product=SJ&p_theme=realcities&p_action=search&p_max docs=200&p_text_search-0=Tech%20AND%20security%20AND%20has%20AND%20a% 20AND%20weak%20AND%20link&s_dispstring=Tech%20security%20has%20a%20wea k%20link%20AND%20date(last%20180%20days)&p_field_date-0=YMD_date&p_ params_date-0=date:B,E&p_text_date-0=-180qzD&p_perpage=10&p_sort=YMD_ date:D&xcal_useweights=no. Internet. Accessed 3 December 2004.

Schneier, Bruce. "Internet Worms and Critical Infrastructure." *CNET News.com* 9 December 2003. Journal on-line. Available from http://news.com.com/2010-7343_3-5117862.html. Internet. Accessed 27 January 2004.

Sullivan, Andy. "U.S. Homeland Chief Urges SEC Cybersecurity Filings." Reuters via USA Today Tech 9 October 2003. Journal on-line. Available from http://www.usatoday.com/ tech/news/computersecurity/2003-10-09-sec-cyberfiling-idea_x.htm. Internet. Accessed 27 January 2004.

Terrorism Research Center, Inc. Definition of cyberterror attributed to the FBI 6 December 2003. Available from http://www.terrorism.com/modules.php?op=modload&name= News&file=article&sid=10145. Internet. Accessed 6 December 2003.

Verton, Dan. "Interview: Outflanking the Cyberterrorist Threat." CNN.com 11 April 2002. Journal on-line. Available from http://www.cnn.com/2002/TECH/industry/04/11/ interview.cybersecurity.idg/. Internet. Accessed 22 September 2003.

Webb, Cynthia L. "Cybersecurity Talk is Cheap." *Washingtonpost.com* 3 December 2003. Journal on-line. Available from http://www.washingtonpost.com/ac2/wp-dyn/A31089-2003Dec3?language=printer. Internet. Accessed 3 December 2003.

Wong, Choon Mei. "Fight Looms over Control of Internet." *Yahoo! News Technology – Reuters Internet Report* 16 September 2003. Journal on-line. Available from http://in.tech.yahoo.com/030916/137/27t9d.html. Internet. Accessed 27 January 2004.